

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **09062596 A**(43) Date of publication of application: **07.03.97**

(51) Int. Cl. **G06F 13/00**
G09C 1/00
G09C 1/00
G09C 1/00
H04L 9/32
H04L 12/54
H04L 12/58

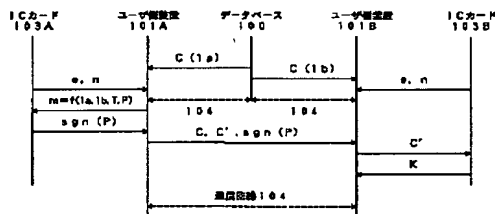
(21) Application number: **07217678**(71) Applicant: **HITACHI LTD**(22) Date of filing: **25.08.95**(72) Inventor: **NISHIOKA GENJI**(54) **ELECTRONIC MAIL SYSTEM**

COPYRIGHT: (C)1997,JPO

(57) Abstract:

PROBLEM TO BE SOLVED: To improve the security related to transmission/reception of electronic mails.

SOLUTION: This system consists of a data base 100 where the public key of each user is registered, at least two information processors 101a and 101b, and IC cards 103a and 103b. Secret keys of users carrying IC cards 103a and 103b and the public key of an authenticating station are stored in memories of IC cards 103a and 103b. In a transmission source A (information processor 101a), its own secret key stored in the memory is used in the IC card 103a to generate a digital signature for transmission data which includes mail data P, user information Ia for discrimination of the transmission source A, user information for discrimination of a transmission destination B, and time information T specifying the transmission date. In a reception side B (information processor 101b), the transmission source, the destination, and the generation date of the electronic mail are verified based on the digital signature included in the received electronic mail.



(11)特許出願公開番号

特開平9-62596.

(43)公開日 平成9年(1997)3月7日

(51)Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 13/00	3 5 1		G 0 6 F 13/00	3 5 1 G
G 0 9 C 1/00	6 3 0	7259-5 J	G 0 9 C 1/00	6 3 0 D
		7259-5 J		6 3 0 F
	6 4 0	7259-5 J		6 4 0 B
	6 6 0	7259-5 J		6 6 0 A
<div style="text-align: right;"> 審査請求 未請求 請求項の数19 O L (全 16 頁) 最終頁に続く </div>				

(21)出願番号 特願平7-217678

(22)出願日 平成7年(1995)8月25日

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72)発明者 西岡 玄次

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

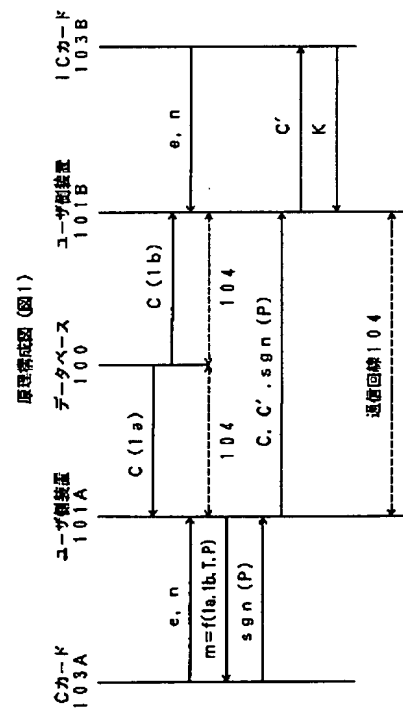
(74)代理人 弁理士 富田 和子

(54) 【発明の名称】 電子メールシステム

(57) 【要約】

【目的】電子メールの送受信に関するセキュリティの向上を図る。

【構成】本システムは、各ユーザの公開鍵が登録されたデータベース１００と少なくとも２台の情報処理装置１０１ａ、１０１ｂとＩＣカード１０３ａ、１０３ｂから構築される。各ＩＣカード１０３ａ、１０３ｂのメモリにはこれを所持するユーザの秘密鍵と認証局の公開鍵が格納されている。送信元Ａ（情報処理装置１０１ａ）では、ＩＣカード１０３ａの内部で、メモリに格納された自己の秘密鍵を用いて、メールデータＰと送信元Ａを識別するためのユーザ情報Ｉａと送信先Ｂを識別するためのユーザ情報と送信日時を特定する時間情報Ｔとを含む送信データに対するデジタル署名を作成する。受信側Ｂ（情報処理装置１０１ｂ）は、受信した電子メールに含まれるデジタル署名を基に、電子メールの送信元、宛先、作成日時を検証する。



1

【特許請求の範囲】

【請求項1】送信元の秘密鍵によりデジタル署名を作成する作成手段と、前記作成手段が作成したデジタル署名を、送信する電子メールのメールアドレスに付加して送信する送信手段とを備える電子メール送信装置であって、前記作成手段は、前記送信元の公開鍵で前記電子メールの送信元と送信先とを検証できるように、前記送信元の秘密鍵により、前記送信元で作成されたメールアドレスと前記送信元を特定するユーザ情報と前記電子メールの送信先を特定するユーザ情報とを含んだ情報に対して、前記デジタル署名を作成することを特徴とする電子メール送信装置。

【請求項2】請求項1記載の電子メール送信装置であって、前記電子メールを複数の送信先に対して送信する場合、前記作成手段は、前記送信元で作成されたメールアドレスと、前記送信元を特定するユーザ情報と、前記各送信先を特定する複数のユーザ情報とを含んだ情報に対して、前記デジタル署名を作成することを特徴とする電子メール送信装置。

【請求項3】請求項1または2記載の電子メール送信装置であって、前記作成手段は、前記情報に含まれるメールアドレスと各ユーザ情報とを接続した接続データを作成する接続手段と、前記接続手段が作成した接続データをハッシュ関数に従って圧縮するハッシュ計算手段と、前記ハッシュ計算手段が圧縮した接続データに対して、前記デジタル署名を作成するデジタル署名作成手段とを備えることを特徴とする電子メール送信装置。

【請求項4】請求項1または2記載の電子メール送信装置であって、前記情報は、更に、前記デジタル署名により前記電子メールの送信日時を検証できるように、前記電子メールの送信日時を特定する時間情報を含むことを特徴とする電子メール送信装置。

【請求項5】請求項4記載の電子メール送信装置であって、前記作成手段は、前記情報に含まれるメールアドレスと各ユーザ情報と前記電子メールの送信日時を特定する時間情報とを接続した接続データを作成する接続手段と、前記接続手段が作成した接続データをハッシュ関数に従って圧縮するハッシュ計算手段と、前記ハッシュ計算手段が圧縮した接続データに対して、前記デジタル署名を作成するデジタル署名作成手段を備えることを特徴とする電子メール送信装置。

【請求項6】請求項3、4または5記載の電子メール送信装置であって、電子メール送信装置は、

2

前記送信手段と、前記接続手段と、前記ハッシュ計算手段とを含んだ本体装置と、

前記送信元のパスワードで暗号化した送信元の秘密鍵の暗号文を記憶するメモリと、前記メモリに記憶された秘密鍵の暗号文を送信元のパスワードで復号する復号手段と、前記デジタル署名作成手段とを内蔵する、前記本体装置に着脱可能なICカードとにより構成され、前記デジタル署名作成手段は、前記復号手段で復合された送信元の秘密鍵により、前記デジタル署名を作成することを特徴とする電子メール送信装置。

【請求項7】送信元の秘密鍵により作成されたデジタル署名を含む電子メールを受信する電子メール受信装置であって、

前記電子メールは、前記電子メールの送信元で作成されたメールアドレスと前記送信元を特定するユーザ情報と前記電子メールの1以上の送信先を特定するユーザ情報とを含んだ情報に対して作成されたデジタル署名を含み、当該電子メール受信装置は、前記デジタル署名と前記送信元の公開鍵とにより、前記電子メールの送信元と送信先とを検証する検証手段を備えることを特徴とする電子メール受信装置。

【請求項8】請求項7記載の電子メール受信装置であって、

前記電子メールは、送信日時を特定する時間情報を加えた情報に対して作成されたデジタル署名を含み、前記検証手段は、前記デジタル署名と前記送信元の公開鍵とにより、更に、前記電子メールの送信日時を検証することを特徴とする電子メール受信装置。

【請求項9】請求項1、2、または3記載の電子メール送信装置と、請求項7記載の電子メール受信装置とを備えることを特徴とする電子メールシステム。

【請求項10】請求項4または5記載の電子メール送信装置と、請求項8記載の電子メール受信装置とを備えることを特徴とする電子メールシステム。

【請求項11】請求項9または10記載の電子メールシステムであって、

前記電子メール送信装置は、前記送信手段と前記接続手段と前記ハッシュ計算手段とを含む本体装置と、前記本体装置に着脱可能なICカードとから構成され、前記電子メール受信装置は、前記検証手段を含む本体装置と、前記本体装置に着脱可能なICカードとから構成され、当該電子メールシステムは、前記電子メール送信装置のICカードと前記電子メール受信装置のICカードを作成すると共に、自身の秘密鍵で暗号化したユーザの公開鍵の暗号文を登録したデータベースを有するデータベースサーバを備えた認証局を備

え、
前記電子メール受信装置の IC カードと前記電子メール送信装置の IC カードは、それぞれ、
前記 IC カードのユーザのパスワードで暗号化された前記 IC カードのユーザの秘密鍵の暗号文と、前記認証局の公開鍵とを記憶するメモリと、
前記メモリに記憶された認証局の公開鍵で、前記認証局のデータベースサーバのデータベースに登録された前記 IC カードのユーザの公開鍵の暗号文を復号する公開鍵復号手段と、
前記 IC カードのユーザから入力された前記 IC カードのユーザのパスワードで、前記メモリに格納された秘密鍵の暗号文を復号する秘密鍵復号手段とを内蔵することを特徴とする電子メールシステム。

【請求項 1 2】自身の秘密鍵で暗号化した、ユーザの公開鍵を含む情報の暗号文を、ユーザの要求に応じてユーザに報告する認証局を備える電子メールシステムにおいて、前記認証局の公開鍵を管理する鍵管理方法であつて、

前記認証局が、前記認証局の公開鍵と前記ユーザのパスワードで暗号化された前記ユーザの秘密鍵の暗号文とを格納したメモリと、入力された前記ユーザのパスワードで前記メモリに格納された秘密鍵の暗号文を復号する第一の復号手段とを内蔵する IC カードを作成するステップと、

前記ユーザの秘密鍵の正当性を検証できるように、前記 IC カードに対する前記ユーザの操作に応じて、前記第一の復号手段が、入力された前記ユーザのパスワードで前記メモリに格納された前記ユーザの秘密鍵の暗号文を復号した前記ユーザの秘密鍵を出力するステップとを有することを特徴とする鍵管理方法。

【請求項 1 3】自身の秘密鍵で暗号化した、ユーザの公開鍵を含む情報の暗号文を、ユーザの要求に応じてユーザに報告する認証局を備える電子メールシステムにおいて、前記認証局の公開鍵を管理する鍵管理方法であつて、

前記認証局は、受付けた各ユーザの公開鍵の暗号文を含むユーザ情報を登録するデータベースを有するデータベ

$$s g n (P) = m_1^{e_1} \bmod n_1 \quad \cdots \text{数式 2}$$

により前記デジタル署名 $s g n (P)$ を作成し、

前記送信手段は、

前記作成手段が作成したデジタル署名 $s g n (P)$ と、ランダムに作成されたデータ暗号化鍵 K で、

【数 3】

$$C_2 = K^{e_2} \bmod n_2 \quad \cdots \text{数式 4}$$

により暗号化された前記データ暗号化鍵 K の暗号文 C_2 とを含んだ前記電子メールを、前記送信先に送信することを特徴とする電子メール送信装置。

ースサーバを備え、

当該鍵管理方法は、

前記認証局が、前記認証局の公開鍵と前記ユーザのパスワードで暗号化された前記ユーザの秘密鍵の暗号文とを格納したメモリと、入力された前記ユーザのパスワードで前記メモリに格納された秘密鍵の暗号文を復号する第一の復号手段と、前記メモリに格納された認証局の公開鍵で前記データベースに登録された前記ユーザの公開鍵の暗号文を復号する第二の鍵復号手段とを内蔵する IC

10 カードを作成すると共に、前記認証局の秘密鍵で暗号化した前記ユーザ情報の暗号文を前記データベースサーバのデータベースに登録するステップと、

前記ユーザの秘密鍵の正当性を検証できるように、前記 IC カードに対する前記ユーザの操作に応じて、入力された前記ユーザのパスワードで、前記第一の復号手段が、前記メモリに格納された前記ユーザの秘密鍵の暗号文を復号した前記ユーザの秘密鍵を出力するステップと、

20 前記ユーザの公開鍵の正当性を検証できるように、前記第二の復号手段が、前記メモリに格納された認証局の公開鍵で前記データベースに登録された前記ユーザの公開鍵の暗号文を復号した前記ユーザの公開鍵を出力するステップとを有することを特徴とする鍵管理方法。

【請求項 1 4】請求項 3 記載の電子メール送信装置であつて、

前記運接手段は、前記メールデータ P と、前記各ユーザ情報とを接続した接続データ m を作成し、

前記ハッシュ計算手段は、前記接続データ m をハッシュ関数 f に従つて、

30 【数 1】

$$m_1 = f (m) \quad \cdots \text{数式 1}$$

により圧縮した圧縮データ m_1 を作成し、

前記デジタル署名作成手段は、前記送信元の秘密鍵と d_1 と公開鍵 (e_1, n_1) とで、前記ハッシュ計算手段が作成した圧縮データ m_1 に対して、

【数 2】

$$C_1 = E (K : P) \quad \cdots \text{数式 3}$$

により暗号化されたメールデータ P の暗号文 C_1 と、前記送信先の公開鍵 (e_2, n_2) で、

【数 4】

$$\cdots \text{数式 4}$$

【請求項 1 5】請求項 1 4 記載の電子メール送信装置であつて、

50 前記送信する電子メールは、更に、前記電子メールの送

信日時を特定する時間情報Tを含み、
前記情報は、更に、前記デジタル署名 $\text{sgn}(P)$ により前記電子メールの送信日時を検証できるように、前記電子メールの送信日時を特定する時間情報Tを含み、
前記接続手段は、前記情報に含まれる前記メールアドレスPと各ユーザ情報と前記時間情報Tとを接続した接続データmを作成することを特徴とする電子メール送信装置。

【請求項16】請求項7記載の電子メール受信装置であ

$$C_2 = K^{e_2} m \text{ mod } n_2 \quad \dots \text{数式 6}$$

により暗号化されたデータ暗号化鍵Kの暗号文 C_2 と、
前記送信元を特定するユーザ情報と前記電子メールの1以上の送信先を特定するユーザ情報とメールアドレスPを含んだ情報に対して作成されたデジタル署名 $\text{sgn}(P)$ とを含み、

$$K = C_2^{d_2} m \text{ mod } n_2 \quad \dots \text{数式 7}$$

により復号する第一の復号手段と、
前記受信した電子メールに含まれる前記メールアドレスPの暗号文 C_1 を、第一の復号手段で復号された前記データ暗号化鍵Kで、

$$P = D(K : C_1) \quad \dots \text{数式 8}$$

により復号する第二の復号手段と、
前記第二の復号手段で復号されたメールアドレスPと各ユ

$$f(m) \equiv \text{sgn}(P)^{e_1} (m \text{ mod } n_1) \quad \dots \text{数式 9}$$

により検証することを特徴とする電子メール受信装置。

【請求項17】請求項16記載の電子メール受信装置であって、

前記受信した電子メールは、前記デジタル署名により前記電子メールの送信日時を検証できるように、更に前記電子メールの送信日時を特定する時間情報Tを含んだ情報に対して作成されたデジタル署名を含むと共に、更に、前記受信した電子メールの送信日時を特定する時間情報Tを含み、

前記接続手段は、前記電子メールのメールアドレスPと各ユーザ情報と時間情報Tとを接続した接続データmを作成することを特徴とする電子メール受信装置。

【請求項18】請求項14記載の電子メール送信装置と、
請求項16記載の電子メール受信装置とを備えることを特徴とする電子メールシステム。

【請求項19】請求項15記載の電子メール送信装置と、

請求項17記載の電子メール受信装置とを備えることを特徴とする電子メールシステム。

【発明の詳細な説明】

って、
前記受信した電子メールは、
ランダムに作成されたデータ暗号化鍵Kで、

$$C_1 = E(K : P) \quad \dots \text{数式 5}$$

により暗号化されたメールアドレスPの暗号文 C_1 と、
前記送信先の公開鍵 (e_2, n_2) で、

$$n_2 \quad \dots \text{数式 6}$$

当該電子メール受信装置は、
前記受信した電子メールに含まれる前記データ暗号化鍵Kの暗号文 C_2 を、前記送信先の秘密鍵 d_2 と公開鍵 (e_2, n_2) とで、

$$\dots \text{数式 7}$$

ユーザ情報とを接続した接続データmを作成する接続手段とを備え、

前記検証手段は、前記受信した電子メールの送信元と送信先とを、前記受信した電子メールに含まれるデジタル署名 $\text{sgn}(P)$ と、前記接続手段が作成した接続データmと、ハッシュ関数fと、送信元の公開鍵 (e_1, n_1) で、

$$\dots \text{数式 9}$$

【0001】

【産業上の利用分野】本発明は、電子メールの送受信に関するセキュリティを管理する電子メール暗号システムに関する。

【0002】

【従来の技術】Internetでの電子メールの送受信に関するセキュリティを管理するための方法として、Linn, J., et, al, Privacy Enhancement Mail for Internet Electronic Mail: Part I, II, III, IV, REF-1421-1424, 1993記載のPEM (Privacy Enhancement Mail) が知られている。これは、米国内務省標準局により標準の暗号化方式として公表されたDESで暗号化したメールアドレスに、RSAに基づいて作成した送信元を識別するためのデジタル署名を付与することにより、電子メールの送受信に関するセキュリティの向上を図るものである。以下、この詳細について説明する。なお、RSAについてはR. L. Rivest, A. Shamir, L. Adleman, . A Method for Obtaining Digital

Signatures and Public Key Cryptosystems, Communications of The ACM, Vol. 21, 1978に、また、DESについてはData Encryption Standard, FIPS-UB-46, 19773に、各々、詳細が記載されている。

【0003】最初に、PEMによる管理下における、電子メールの送受信に関する一連の処理（後述）において使用される公開鍵（ e, n ）について説明する。

【0004】PEMを利用する各ユーザには、それぞれ、公開鍵（ e, n ）が割り当てられている。そして、PEMの正当な各ユーザには、認証局固有の公開鍵（ e', n' ）が正当な手段により教示される。また、こうしたユーザには、それぞれ、そのユーザの公開鍵（ e, n ）等の、PEMによる管理下において電子メールの送受信を行うために必要とされる情報を認証局の秘密鍵 d' で暗号化した暗号文が記載された公開鍵証明書が、一種の身分証明書として発行される。

【0005】次に、このような公開鍵（ e, n ）を利用した、PEMの管理下における、電子メールの送受信に関する一連の処理について説明する。ただし、電子メールの送信元Aと送信先Bは、正当な手段により認証局に登録されたユーザ同士であり、事前に、互いに相手の公開鍵証明書を正当な手段（例えば、互いに公開鍵証明書を送付し合う等）で獲得していることを前提とする。

【0006】まず、電子メールの送信元Aでの処理について説明する。

$$sgn_1(P) = f(P)^{e_1} \pmod{n_1} \quad \cdots \text{数式 1 2}$$

【0014】ここで、 $f(P)$ は、データを圧縮するハッシュ関数である。なお、このハッシュ関数 f は、PEMの管理下において、一般に公開される情報に含まれる関数である。

【0015】ここまでの処理が完了したら、送信元Aは、送信先Bへ、 $C_1, C_2, sgn_1(P)$ を電子メールとして送信する。

【0016】次に、この電子メールの送信先Bにおいて電子メールが受信された場合の処理について説明する。ただし、電子メールを受信した後から、送信先Bを受信側Bと呼び替えるものとする。

【0017】送信先Bにおいて送信元Aからの電子メールが受信されると、受信側Bでは、まず、自身Bの公開鍵（ e_2, n_2 ）と秘密鍵 d_2 を併用して、数式13に基づく処理を施すことにより、受信した電子メールに含まれる C_2 を復号してデータ暗号化鍵 K を得た後、更に、このデータ暗号化鍵 K を使用して、数式14に基づく処理を施すことにより、電子メールに含まれる C_1 を復号してメールアドレス P を得る。

【0018】

【0007】さて、送信元Aでは、まず、作成したメールアドレス P を暗号化するためのデータ暗号化鍵 K を任意に作成する。そして、この鍵暗号 K を使用し、次式に基づいて、DESによる暗号化処理をメールアドレス P に対して施すことにより、メールアドレスの暗号文 C_1 を作成する。

【0008】

$$C_1 = E(K : P) \quad \cdots \text{数式 1 0}$$

10 【0009】ここで、 $E(K : P)$ は、鍵暗号 K でメールアドレス P を暗号化するための関数である。

【0010】また、認証局の公開鍵（ e', n' ）を使用して、事前に獲得しておいた送信先Bの公開鍵証明書に記載された暗号文から送信先Bの公開鍵（ e_2, n_2 ）を復号する。更に、得られた送信先Bの公開鍵（ e_2, n_2 ）を使用して、次式に基づくRSAによる暗号化処理をデータ暗号化鍵 K に施すことにより、データ暗号化鍵 K の暗号文 C_2 を作成する。

【0011】

$$20 \quad C_2 = K^{e_2} \pmod{n_2} \quad \cdots \text{数式 1 1}$$

【0012】そして、送信元Aは、自身の秘密鍵 d_1 と公開鍵（ e_1, n_1 ）とを併用し、メールアドレス P の作成者が自身であることを証明するためのデジタル署名 $sgn_1(P)$ を次式に基づいて作成する。

【0013】

【数12】

【数13】

$$K = C_2^{d_2} \pmod{n_2} \quad \cdots \text{数式 1 3}$$

【0019】

【数14】

$$P = D(K : C_1) \quad \cdots \text{数式 1 4}$$

【0020】ここで、 $D(K : C_1)$ は、データ暗号化鍵 K で、電子メールに含まれる C_1 を復号する関数である。

40 【0021】そして、このメールアドレス P の作成者と電子メールの送信元とが同一であることを検証するため、すなわち、電子メールに含まれたデジタル署名 $sgn_1(P)$ が確かに電子メールの送信元Aにより作成されたものであることを検証するために、数式14により得られたメールアドレス P と、電子メールの送信元Aの公開鍵（ e_1, n_1 ）とが次式の関係を満足することを確認する。万が一、数式14により得られたメールアドレス P と、電子メールの送信元Aの公開鍵（ e_1, n_1 ）とが次式の関係を満足しないならば、メールアドレス P の作成者

とこの電子メールの送信元とが異なるユーザであることになり、何者かによりメールアドレスPが不当に改竄されている可能性を疑う必要がある。

$$f(P) \equiv \text{sgn}_1(P)^{e_1} \pmod{n_1} \quad \cdots \text{数式 15}$$

【0023】なお、ここで使用する電子メールの送信元Aの公開鍵(e_1, n_1)は、認証局の公開鍵(e', n')を使用して、送信元Aの公開鍵証明書に記載された暗号文を復号することにより得られたものである。

【0024】このように、PEMによる管理下で電子メールの送受信を行えば、盗聴や内容改竄等の不正な行為を防止することができる。

【0025】

【発明が解決しようとする課題】ところが、上記PEMでは、電子メールの送信元AにおいてメールアドレスPの作成者を識別するためのデジタル署名 $\text{sgn}_1(P)$ は付与されるけれども、メールアドレスPがいつれのユーザに宛てて作成されたものであるかを識別するための情報は付与されないため、電子メールの受信側Bにおいては、受信した電子メールに含まれているメールアドレスPが、確かに自身に宛て作成されたものであるということの確証をつかむことができない。すなわち、メールアドレスの内容が改竄されていなければ、同一の作成者により作成された別のメールアドレスによって、メールアドレスの内容がすり替えられていても、受信側ではこれを検知できないという問題があった。例えば、電子メールの受信側Bが、受信した電子メール(何らかの提案Cに対して賛否を問う内容のメールアドレス)に対する応答文P(賛成である旨を記載したもの)を作成し、これにデジタル署名 $\text{sgn}_1(P)$ を付与して、送信先Aに電子メールとして返送した場合に、不正者が、誤った情報を流す目的をもって、以前にBから送信されたデジタル署名付きの電子メールのメールアドレスの内から、応答文として悪用できる内容のメールアドレス P_1 (反対である旨を記載したもの)を不正に使用して、電子メールのメールアドレスのすり替えを行っても、これを受信したAでは、メールアドレス P_1 に付与されたデジタル署名 $\text{sgn}_1(P_1)$ により、確かにBからの応答文であることを確認して、その内容を信頼することになる。

【0026】また、上記PEMによる管理下では、個々のユーザの公開鍵については、認証局が発行した公開鍵証明書によってそれが正当なものであることが証明されるが、認証局自体の公開鍵については、個々のユーザ側からそれが正当なものであるかどうかを確認することができない。こうしたことが、PEMを利用するユーザが、不正なユーザの不正行為による被害を被る原因となる可能性は高い。例えば、不正なユーザが、認証局の公開鍵を偽って、認証局になりすますという可能性がある。

【0027】そこで、本発明は、電子メールの送受信に

【0022】

【数15】

関するセキュリティの向上を図るために適した電子メール暗号システムを提供することを目的とする。

【0028】

【課題を解決するための手段】上記目的達成のために、本発明は、送信元の秘密鍵によりデジタル署名を作成する作成手段と、前記作成手段が作成したデジタル署名を、送信する電子メールのメールアドレスに付加して送信する送信手段とを備える電子メール送信装置であって、前記作成手段は、前記送信元の公開鍵で前記電子メールの送信元と送信先とを検証できるように、前記送信元の秘密鍵により、前記送信元で作成されたメールアドレスと前記送信元を特定するユーザ情報と前記電子メールの送信先を特定するユーザ情報とを含んだ情報に対して、前記デジタル署名を作成することを特徴とする電子メール送信装置を提供する。

【0029】更に、送信元の秘密鍵により作成されたデジタル署名を含む電子メールを受信する電子メール受信装置であって、前記電子メールは、前記電子メールの送信元で作成されたメールアドレスと前記送信元を特定するユーザ情報と前記電子メールの1以上の送信先を特定するユーザ情報とを含んだ情報に対して作成されたデジタル署名を含み、当該電子メール受信装置は、前記デジタル署名と前記送信元の公開鍵とにより、前記電子メールの送信元と送信先とを検証する検証手段を備えることを特徴とする電子メール受信装置を提供する。

【0030】そして、こうした電子メール送信装置と電子メール受信装置とを備えた電子メールシステムを提供する。

【0031】

【作用】本発明に係る電子メール送信装置によれば、前記作成手段は、前記送信元で作成されたメールアドレスと前記送信元を特定するユーザ情報と前記電子メールの送信先を特定するユーザ情報とを含んだ情報に対して、前記送信元の公開鍵で前記電子メールの送信元と送信先との検証が可能な前記デジタル署名を作成する。

【0032】また、本発明に係る電子メール受信装置によれば、前記検証手段は、前記受信した電子メールに含まれるデジタル署名と、前記送信元の公開鍵とにより、前記電子メールの送信元と送信先とを検証する。

【0033】そして、本発明に係る電子メールシステムは、こうした電子メール送信装置と電子メール受信装置とから構築されるので、電子メール受信装置側では、前記電子メール送信装置側で付与されたデジタル署名により、受信した電子メールの送信元と宛先とを確認することができる。従って、不正なユーザによるメールアドレス

のすり替え等を防止することができる。その結果、各装置の間で送受信される電子メールの機密性が保持される。

【0034】また、電子メールシステムの構成として、各ユーザの公開鍵の暗号文を含むユーザ情報を登録するデータベースを有するデータベースサーバを備えた認証局を加えて、この認証局により各ユーザの公開鍵を一元的に管理するようにすれば、従来PEMにおいて不明確であった認証局の公開鍵の正当性を容易に確認することができる。すなわち、認証局は、各ユーザから受付け、各ユーザの公開鍵を含むユーザ情報を、自身の秘密鍵で暗号化してデータベースに登録すると共に、認証局の公開鍵を格納したメモリを内蔵するICカードを作成する。一方、認証局からICカードを受け取った各ユーザは、認証局のデータベースにアクセスして自身のユーザ情報の暗号文を取得することにより、まず、自身が、本システムを利用するユーザとして正式に登録されているかを確認する。更に、ICカードのメモリに格納された認証局の公開鍵で、認証局のデータベースにアクセスして取得した自身のユーザ情報の暗号文を復号し、このユーザ情報に含まれる公開鍵の正当性を確認する。このとき、万一、このユーザ情報に含まれる公開鍵の正当性が確認できなければ、ユーザの登録の段階で認証局のなりすまし等の不正が行われたことが裏付けられたことになる。このように認証局のデータベースによって各ユーザの公開鍵を一元的に管理し、かつ、ICカードにより認証局の公開鍵の安全性を確保するようにすれば、認証局の公開鍵の正当性が保証され、システム全体のセキュリティが確保される。

【0035】更に、このICカードのメモリにユーザの秘密鍵を格納すると共に、このICカードの内部で、ユーザの秘密鍵を用いるデジタル署名を作成する際の処理の実行を可能とすれば、ユーザの秘密鍵の機密性も同時に保持することができるので、システム全体のセキュリティを一層向上させることができる。

【0036】

【実施例】以下、添付の図面を参照しながら、本発明に係る実施例について説明する。

【0037】まず、図1を参照しながら、本実施例に係るシステムの基本的な構成について説明する。以下、秘密鍵暗号方式としてDESを用いる場合を一例に挙げて説明するが、本システムにおける秘密鍵暗号方式は、必ずしもこれである必要はない。例えば、FEAL等の、他の方式を用いても構わない。

【0038】本システムは、図1に示すように、従来技術の欄で説明した認証局に相当する情報処理装置100と、少なくとも2台の情報処理装置101a、101bと、メールデータに付与するデジタル署名の作成処理等を行なうICカード103a、103bとにより構築される。ただし、2台の情報処理装置101a、101b

の間と、各報処理装置100、101a、101bの間は、相互にデータの転送が行なえるように、各々通信回線104で接続されている。また、各情報処理装置101a、101bは、装着したICカード103a、103bとの間で、相互にデータの入出力を行なうことができる。

【0039】これらの情報処理装置101a、101bは、それぞれ、図2に示すように、作成したメールデータ等を表示する表示装置201a、201bと、ICカード103a、103b用のI/Oポート202a、202bと、RSAによる暗号処理を行なうRSA暗号処理部203a、203bと、DESによる暗号処理を行なうDES暗号処理部204a、204bと、メモリ205a、205bと、乱数を発生する乱数発生部206a、206bと、乱数発生部206a、206bが発生する乱数から鍵暗号Kを作成する鍵生成部207a、207bと、ハッシュ関数によりデータを圧縮するハッシュ計算部208a、208bと、メールデータに付与されたデジタル署名を検証するデジタル署名検証部209a、209bと、通信回線104で相互に接続された他の情報処理装置との間の通信の制御する通信制御部210a、210bと、メールデータ等を入力する入力装置(キーボード等)(不図示)とを備える。そして、これら各ブロック間のデータ転送はバス212を介して行なわれる。なお、この構成は、ハードウェアと、CPUにより実現されるプロセスとを機能的に示したものである。

【0040】一方、ICカード103a、103bは、装着された情報処理装置101a、101bからのデータの入力を制御する入力部301a、301bと、バスワードから鍵暗号化鍵 K_1 を作成する鍵暗号生成部302a、302bと、認証局の公開鍵(e' 、 n')等を格納するメモリ303a、303bと、DESによる暗号処理を行なうDES暗号処理部304a、304bと、RSAによる暗号処理を行なうRSA暗号処理部305a、305bと、デジタル署名を作成するデジタル署名作成部306a、306bと、装着された情報処理装置101a、101bへのデータの出力を制御する出力部307a、307bとを備える。なお、この構成は、ハードウェアと、CPUにより実現されるプロセスとを機能的に示したものである。

【0041】以上で、本システムの構成についての説明を終わる。

【0042】次に、このように構築されたシステムの管理下で行なわれる、電子メールの送受信に関する処理について説明する。

【0043】最初に、ユーザが本システムを利用するための前提として行う、情報処理装置100のデータベースへの登録処理について説明する。

【0044】まず、本システムを利用とするユーザは、各々、次式を満足するように、自身の公開鍵(e 、 n)と

秘密鍵 d とを任意に作成する。ただし、 e と n は整数であり、 p と q は、RSA による暗号化において機密性が確保される程度に大きな、互いに異なる値を有する素数である。なお、以下、対応する公開鍵と秘密鍵は、全て、これと同様な関係を満足するように作成されたものであることを前提とする。

$$e \cdot d = 1 \pmod{1 \cdot c \cdot d \cdot (p-1, q-1)}$$

…数式 1 7

【0047】ただし、上式において、 $1 \cdot c \cdot d \cdot (p-1, q-1)$ は、2つの整数 $p-1, q-1$ の最小公倍数を意味する。

【0048】次に、自身のパスワード s を任意に作成し、これを次式に基づいて暗号化して、鍵暗号化鍵 K_1 を作成する。

【0049】

【数18】

$$K_1 = F(s) \quad \dots \text{数式 1 8}$$

【0050】ここで、 $F(s)$ は、従来技術の欄で説明した PEM の管理下において公開される情報に含まれる周知の鍵生成関数である。

【0051】更に、この鍵暗号化鍵 K_1 を使用して、次式に基づく DES による暗号化処理を秘密鍵 d に施すことにより、秘密鍵 d の暗号文 C を作成する。

【0052】

【数19】

$$C(I_1) = I_1^{d'} \pmod{n'} \quad \dots \text{数式 2 0}$$

【0056】さて、こうして情報処理装置 100 のデータベースに登録された各ユーザには、それぞれ、自身の秘密鍵 d_1 の暗号文 C_1 と認証局の公開鍵 (e', n') とが格納されたメモリ 303 を内蔵する IC カード 103 が配布される。こうした情報処理装置 100 のデータベースへのユーザの登録は、然るべき調査を経た後、信頼のおけるユーザに関してのみ行なわれるものであり、例えば、登録を申請したユーザが自身に関する固有情報を偽る不正な者である場合等には、こうしたユーザは登録対象から除外される。

【0057】ところで、システムの安全上、登録されたユーザの側では、認証局から IC カード 103 が配布された際に、情報処理装置 100 のデータベースにアクセスし、取得した自身のユーザ情報の暗号文 $C(I_1)$ を、配布された IC カード 103 のメモリ 303 に格納された認証局の公開鍵 (e', n') で復号して、このユーザ情報 I_1 に含まれる公開鍵 (e, n) が、申請したものと同じであることを確認することが望まれる。こうした確認を行うことによって、本システムを利用するユーザとしての正当性と、IC カード 103 のメモリ 303 に格納された認証局の公開鍵の正当性が共に保証される。また、これと並行して、各ユーザは、配布された IC カード 103

【0045】

【数16】

$$n = p \cdot q \quad \dots \text{数式 1 6}$$

【0046】

【数17】

$$C = E(K_1; d) \quad \dots \text{数式 1 9}$$

【0053】以上の処理が終了したら、ユーザは、公開鍵 (e, n) と上式により作成した秘密鍵 d の暗号文 C とを情報処理装置 100 へ転送することにより自身の登録を依頼する。このとき、情報処理装置 100 のデータベースに公開鍵 (e, n) と共に登録される固有情報(ユーザ名、メールアドレス等)も転送する。

【0054】一方、これを受け付けた情報処理装置 100 側では、認証局の公開鍵 (e', n') 及び秘密鍵 d' を使用して、転送された固有情報及び公開鍵 (e, n) と、登録の有効期限等の記録した付加情報とを含むユーザ情報 I_1 を次式に基づいて暗号化して暗号文 $C(I_1)$ を作成する。そして、このユーザ情報の暗号文 $C(I_1)$ をデータベースに登録する。

【0055】

【数20】

のメモリ 303 に格納された暗号文 C_1 を自身のパスワードで復号して得られる秘密鍵 d が、申請したものと同一であることを確認することが望ましい。万一、自身のパスワードによる復号が不可能である場合等には、IC カード 103 がユーザの手に渡るまでの間に認証局のなりすまし等の不正が行われた可能性を疑う必要がある。

【0058】以上で、情報処理装置 100 のデータベースへの登録処理についての説明を終わる。

【0059】次に、本システムにおける、電子メールの送受信に関する一連の処理について説明する。ただし、電子メールの送信元 A (情報処理装置 101 a) と送信先 B (情報処理装置 101 b) は、共に、前述した登録処理により、本システムの正当なユーザとして情報処理装置 100 のデータベースに登録された者同士であることを前提とする。また、以下に示す電子メールの送信時及び受信時には、各ユーザ A, B は、既に、情報処理装置 100 のデータベースを検索することによって、互いのユーザ情報の暗号文を獲得しているものとする。

【0060】まず、電子メールの送信元 A で行なわれる処理について説明するが、図 4 に示すように、この処理には、情報処理装置 101 a の備える構成部(図 2 に示した各ブロック)を利用して行なわれるものと、IC カ

15

ード103aの備える構成部(図3に示した各ブロック)を利用して行なわれるものとがあるので、以下、これらを別個に説明していく。

【0061】電子メールの送信元Aは、情報処理装置101aが備える構成を利用して、以下に示す処理を行なう。

【0062】電子メールの送信元Aは、ICカード103a用のI/Oポート202aに接続されたICカード103aのメモリ303aに格納された認証局の公開鍵

$$I' b = C (I b)^{e' m o n n'} \quad \cdots \text{数式 2 1}$$

【0064】

$$I a = C (I a)^{e' m o n n'} \quad \cdots \text{数式 2 2}$$

【0065】なお、得られたユーザ情報Ia及びIbは、この電子メールが送信されるまで間、一旦、メモリ205aに格納される。

【0066】また、DESによる暗号化処理をメールデータPに施して、メールデータPの暗号文C₁を作成する。すなわち、鍵生成部207aにおいて、乱数発生部206aが発生する乱数列を利用する、データ暗号化鍵Kの作成が実行された後、DES暗号処理部304aにおいて、次式に基づくメールデータPの暗号化処理が実行される。

【0067】

【数23】

$$C = E (K : P) \quad \cdots \text{数式 2 3}$$

【0068】なお、作成されたメールデータPの暗号文Cは、この電子メールが送信されるまで間、一旦、メモリ205aに格納される。

【0069】その後、メールデータPの暗号化に使用したデータ暗号化鍵Kを暗号化し、C'を作成する。すなわち、RSA暗号処理部203aにおいて、送信先Bのユーザ情報Ibに含まれる公開鍵(e₂, n₂)を使用した、

$$m = f (z (I a, I b, P, T)) \quad \cdots \text{数式 2 5}$$

【0074】このようにハッシュ関数fの入力データを接続関数zにより与えるのは、ハッシュ関数fの入力データ数が仕様により1に限定されているためである。従って、ハッシュ関数fの入力データは、必ずしも接続関数zにより与える必要はなく、複数のデータを連結することができる他の適当な関数により与えても構わない。ただし、ハッシュ関数に与えられるデータは、一定の処理で、元の複数のデータに分離可能でなければならない。

【0075】ここまでの処理が終了したら、作成した送信データmを、I/Oポート202aを介してICカード103aへと転送する。

【0076】一方、ICカード103aの入力部301aが、情報処理装置101a側から転送された送信デ

16

(e', n')を使用して、送信先Bのユーザ情報の暗号文C(Ib)を復号して送信先Bのユーザ情報Ibを得ると共に、自身Aのユーザ情報の暗号文C(Ia)を復号して自身Aのユーザ情報Iaを得る。すなわち、情報処理装置101aのRSA暗号処理部203aにおいて、次式に基づく復号化処理が実行される。

【0063】

【数21】

【数22】

次式に基づくデータ暗号化鍵Kの暗号化処理が実行される。

【0070】

【数24】

$$C' = K^{e_2 \text{ mod } n_2} \quad \cdots \text{数式 2 4}$$

【0071】なお、作成されたC'は、この電子メールが送信されるまで間、一旦、メモリ205aに格納される。

【0072】以上の処理が終了したら、自身Aのユーザ情報Iaと、送信先Bのユーザ情報Ibと、作成したメールデータPと、現在の日時を特定する時間情報Tとから、送信データmを作成する。すなわち、ハッシュ計算部208aにおいて、次式に基づく圧縮処理が実行され、その結果、送信データmが作成される。ただし、次式において、z(x₁, ..., x_n)は、データx₁, ..., x_nを相互に接続する接続関数であり、可変個数のデータx₁, ..., x_nを入力とする。

【0073】

【数25】

タmを受付けると、ICカード103a側では、この送信データmが一旦メモリ303aに格納された後、以下に示す、デジタル署名の作成処理が開始される。なお、以下、ICカード103aの備える各構成部と情報処理装置101aの備える各構成部との間のデータ転送は、情報処理装置101aの備えるICカード103a用のI/Oポート202aと、ICカード103aの備える入力部301a及び出力部307aを介して行なわれるものとし、送信元Aからの入力は、こうしたデータ転送経路を利用して情報処理装置101aの入力装置からICカード103aの各構成部に転送されるものとする。

【0077】ICカード103aの鍵暗号生成部302aにおいて、送信元Aから入力されたパスワードs₁が暗号化され、鍵暗号化鍵K₁が作成される。すなわち、

20

30

40

50

鍵暗号生成部302aにおいて、次式に基づく暗号処理が実行される。

【0078】

【数26】

$$K_1 = F(s_1) \quad \dots \text{数式 2 6}$$

【0079】ここで、 $F(s)$ は、前述の鍵生成関数である。

【0080】鍵暗号生成部302aで鍵暗号化鍵 K_1 が生成されると、DES暗号処理部304aにおいて、メモリ303aに格納された秘密鍵 d_1 の暗号文 C が、秘密鍵 d_1 に復号される。すなわち、DES暗号処理部304aにおいて、次式に基づく復号処理が実行される。

$$sgn_1(P) = m^{d_1} \bmod n_1 \quad \dots \text{数式 2 8}$$

【0084】ここで、 $f(P)$ は、前述のハッシュ関数である。

【0085】そして、情報処理装置101aへ、デジタル署名作成部206で作成されたデジタル署名 $sgn_1(P)$ が転送されて、ICカード103a側で行なわれるデジタル署名の作成処理は終了する。

【0086】さて、情報処理装置101aのICカード103a用のI/Oポート202aが、ICカード103a側から転送されたデジタル署名 $sgn_1(P)$ を受付けると、情報処理装置101a側では、このデジタル署名 $sgn_1(P)$ を、メモリ205aに格納された C, C', Ia, Ib と共に、電子メールとして送信する。以上で、電子メールの送信元Aで行なわれる処理についての説明を終わる。

【0087】次に、この電子メールが送信先B(情報処理装置101b)で受信された場合に行なわれる処理を、情報処理装置101bの備える構成部(図2に示した各ブロック)で行なわれるものと、ICカード103bの備える構成部(図3に示した各ブロック)で行なわれるものとに分割して説明する。ただし、以下、送信先Bを受信側Bと呼び替えるものとする。

【0088】電子メールの受信側B(情報処理装置101b)で電子メールが受信されると、情報処理装置101b側から、ICカード103b側へと、電子メールに含まれる暗号文 C が転送される。ICカード103bの入力部301bがこれを受け取ると、ICカード103b側では、これを一旦メモリ303bに格納した後、以下に示す処理を実行する。

【0089】鍵暗号生成部302bにおいて、受信側Bから入力されたパスワード s_2 が暗号化されて、鍵暗号化鍵 K_2 が作成される。すなわち、鍵暗号生成部302bにおいて、次式に基づく暗号処理が実行される。

【0090】

【数29】

$$K_2 = F(s_2) \quad \dots \text{数式 2 9}$$

【0091】ここで、 $F(s_2)$ は、前述の鍵生成関数で

【0081】

【数27】

$$d_1 = D(K_1 : C) \quad \dots \text{数式 2 7}$$

【0082】更に、デジタル署名作成部206において、DES暗号処理部304aで復号された秘密鍵 d_1 と、メモリ303aに格納された公開鍵 (e_1, n_1) と、メモリ303aに格納してある送信データ m に対して、デジタル署名 $sgn_1(P)$ が作成される。すなわち、デジタル署名作成部206において、次式に基づく、デジタル署名の作成処理が実行される。

【0083】

【数28】

ある。

【0092】鍵暗号生成部302bで鍵暗号化鍵 K_2 が作成されると、DES暗号処理部304bにおいて、メモリ303bに格納された秘密鍵 d_2 の暗号文 C' が復号される。すなわち、DES暗号処理部304bにおいて、次式に基づく復号処理が実行される。

【0093】

【数30】

$$d_2 = D(K_2 : C) \quad \dots \text{数式 3 0}$$

【0094】DES暗号処理部304bで秘密鍵 d_2 が得られると、RSA暗号処理部305bにおいて、この秘密鍵 d_2 と、受信側Bの公開鍵 (e_2, n_2) とによって、メモリ303bに格納された暗号文 C が復号される。すなわち、RSA暗号処理部305bにおいて次式に基づく復号処理が実行されて、電子メールの送信元Aがメールアドレス P の暗号化に使用したデータ暗号化鍵 K が得られる。

【0095】

【数31】

$$K = C'^{d_2} \bmod n_2 \quad \dots \text{数式 3 1}$$

【0096】ここまでの処理が終了したら、このデータ暗号化鍵 K が情報処理装置101bへと転送されて、ICカード103b側で実行される処理は終了する。

【0097】さて、情報処理装置101bのICカード103b用のI/Oポート202bが、ICカード103b側から転送されたデータ暗号化鍵 K を受付けると、情報処理装置101b側では、このデータ暗号化鍵 K が一旦メモリ205bに格納された後、以下に示すデジタル署名の確認処理が開始される。

【0098】まず、DES暗号処理部204bにおいて、電子メールに含まれるメールアドレス P の暗号文 C が復号される。すなわち、DES暗号処理部204bにおいて、メモリ205bに格納されたデータ暗号化鍵 K を使用した、次式に基づく復号処理が実行される。

10

20

30

40

50

【0099】

【数32】

$$P = D(K : C) \quad \cdots \text{数式 3 2}$$

【0100】そして、デジタル署名検証部209bにおいて、電子メールに含まれるデジタル署名 $sgn_1(P)$ と、ハッシュ計算部208bにおいて作成されるデータ $f(z(P, Ia, Ib, T))$ とが、次式の関係を満足すること

$$f(z(Ia, Ib, P, T))$$

$$\equiv sgn_1(P)^{e_1} \pmod{n_1} \quad \cdots \text{数式 3 3}$$

【0102】この関係を満足すれば、その電子メールの機密性は保たれていることを意味し、反対にこの関係を満足しないならば、何者かによって不当にメールアドレスPの内容が改竄されていることを疑う必要がある。

【0103】本実施例に係るシステムでは、このように、電子メールの送信元Aにおいて、メールアドレスP、電子メールの送信元Aを識別するためのユーザ情報Ia、電子メールの送信先Bを識別するためのユーザ情報、電子メールの送信日時を特定するための時間情報Tを含めた送信データに対してデジタル署名が付与されるため、電子メールの受信側において、電子メールの送信元の検証、電子メールの宛先の検証、電子メールの作成日時の検証を行なうことができる。従って、従来技術の欄で説明したPEMの管理下では起こり得た、不正なユーザによるメールアドレスの内容のすり替え等を防止することができる。すなわち、本実施例に係るシステムによれば、従来技術の欄で説明したPEMよりも多岐に渡って電子メールの機密性を保持することができる。また、認証局の公開鍵(e' , n')及びユーザの秘密鍵dの暗号に係る処理をICカード内部のみで行なうため、これを所持する正当なユーザ以外の者に対する認証局の公開鍵(e' , n')の機密性が保証され、かつ、自身以外のユーザに対する秘密鍵の機密性が保持される。従い、システム全体としての安全性が向上する。

【0104】ところで、本実施例に係るシステムでは、認証局の公開鍵(e' , n')及びユーザの秘密鍵dの機密性を保証するためICカードを使用しているが、必ずしもこれを使用する必要はない。例えば、PEMと同様な公開鍵証明書等を使用しても構わない。ただし、この場合には、認証局の公開鍵(e' , n')及びユーザの秘密鍵dの正当性が確保されるように公開鍵証明書等の配布が充分慎重に行なわれる必要があり、更に、図5に示すように、本システムを構築する情報処理装置には、図3のICカードが備える鍵暗号生成部302と同様な処理を行なう鍵暗号生成部507を新たに付加する必要がある。その代わり、ICカード用のI/Oポートは不要となる。なお、こうした場合には、ICカードのメモリの代用として、自身の秘密鍵d₁の暗号文C₁と認証局の公開鍵(e' , n')とを格納したフロッピディスク等の記憶媒体を利用するようにしても良い。

とが確認される。ただし、Pは、DES暗号処理部204bで得られたメールアドレスであり、Iaは、電子メールの送信元Aのユーザ情報であり、Ibは、自身Bのユーザ情報であり、Tは、電子メールのヘッダに含まれる送信日時を特定する時間情報である。

【0101】

【数33】

【0105】これまで電子メールの送信元と送信先が1対1の場合を例として説明してきたが、電子メールの送信形態には、送信元Aが、同一内容のメールアドレスを含む電子メールを、複数の送信先B₁, ..., B_nに対して同時に送信するというものがある。本実施例に係るシステム下で、こうした電子メールの送信形態をとる場合には、送信元Aにおいて送信データmを作成する際に、ハッシュ関数fに入力データを与える接続関数zの入力データとして、送信元Aのユーザ情報Iaと、全複数の送信先B₁, ..., B_nのユーザ情報Ib₁, ..., Ib_nと、メールアドレスPと、現在の日時を特定する時間情報Tとを与えれば良い(次式参照)。

【0106】

【数34】

$$m = f(P) \quad \cdots \text{数式 3 4}$$

【0107】最後に、本システムとPEMをまたがった電子メールの送受信について説明しておく。こうした場合には、電子メールを送受信するユーザ同士が、互いに、相手の利用するシステムを認識している必要がある。従って、ユーザは、システムへの登録を依頼する際に、自身が利用する電子メールの暗号化方式を特定するための情報(例えば、電子メールの暗号化方式の名称)を含んだ固有情報を送信するようにする。一方、PEMにおいては、認証局は、ユーザが利用する電子メールの暗号化方式を特定するための情報(例えば、PEM等の、電子メールの暗号化方式の名称)を含んだ情報を暗号化した暗号文を記載した公開鍵証明書を発行する。

【0108】さて、本システムの側において、このようにシステムをまたいで相互に電子メールを送受信する場合に対応するためには、数式25及び数式33の接続関数zを、次式を満たすように定めておく必要がある。

【0109】

【数35】

$$z(P) = P \quad \cdots \text{数式 3 5}$$

【0110】そして、本システムを利用するユーザから、PEMを利用するユーザへと電子メールを送信する場合には、次式に基づいて送信データmを作成すれば良い。

【0111】

【数36】

20

30

40

50

$$m = f(z(P)) \quad \dots \text{数式 3 6}$$

【0112】一方、本システムを利用するユーザが、P
EMを利用するユーザからの電子メールを受信した場合
には、次式に基づいて、デジタル署名の確認処理を行え

$$f(z(P)) \equiv \text{sgn}_1(P)^{e_1} \pmod{n_1} \quad \dots \text{数式 3 7}$$

【0114】

【発明の効果】本発明に係る電子メールシステムによれば、電子メールの送受信に関するセキュリティの向上を図ることができる。

【図面の簡単な説明】

【図1】本発明の実施例に係るシステム構成の一例を説明する図である。

【図2】図1の情報処理装置の機能的な構成を説明する図である。

【図3】図1のICカードの機能的な構成を説明する図である。

【図4】本発明の実施例に係るシステムを構成する情報処理装置の機能的な構成の一例を説明する図である。

【図5】本発明の実施例に係るシステムを構成する情報処理装置の機能的な構成の他の一例を説明する図である。

【符号の説明】

100, 101a, 101b…情報処理装置

103a, 103b…ICカード

ばよい。

【0113】

【数37】

104…通信回線

201a, 201b…表示装置

202a, 202b…ICカード用のI/Oポート

10 203a, 203b…RSA暗号処理部

204a, 204b…DES暗号処理部

205a, 205b…メモリ

206a, 206b…乱数発生部

207a, 207b…鍵生成部

208a, 208b…ハッシュ計算部

209a, 209b…デジタル署名検証部

210a, 210b…通信制御部

212…バス

301a, 301b…入力部

20 302a, 302b…鍵暗号生成部

303a, 303b…メモリ

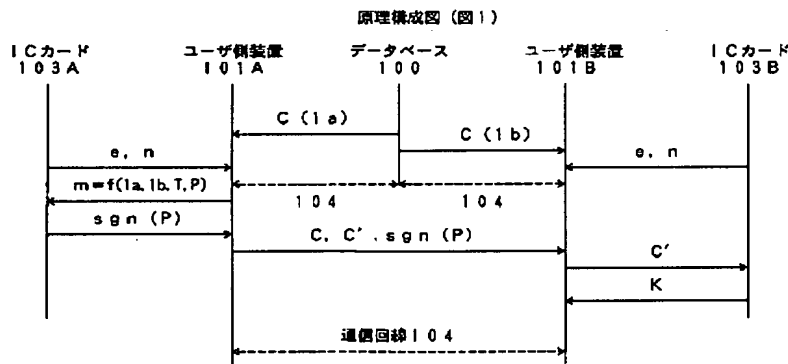
304a, 304b…DES暗号処理部

305a, 305b…RSA暗号処理部

306a, 306b…デジタル署名作成部

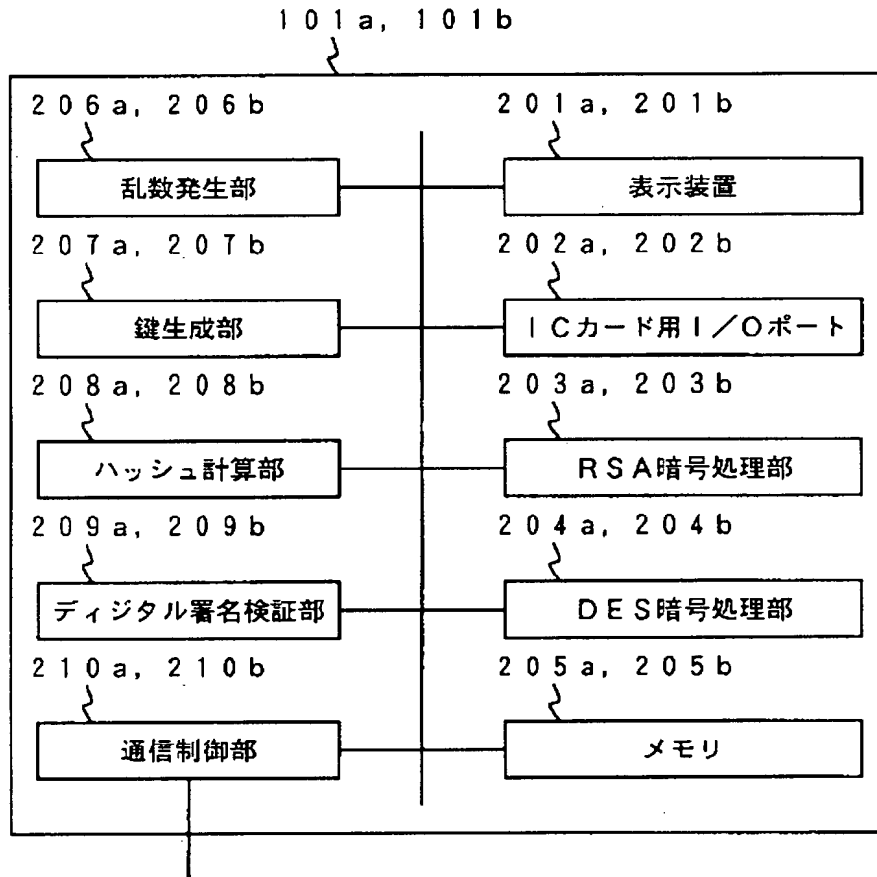
307a, 307b…出力部

【図1】



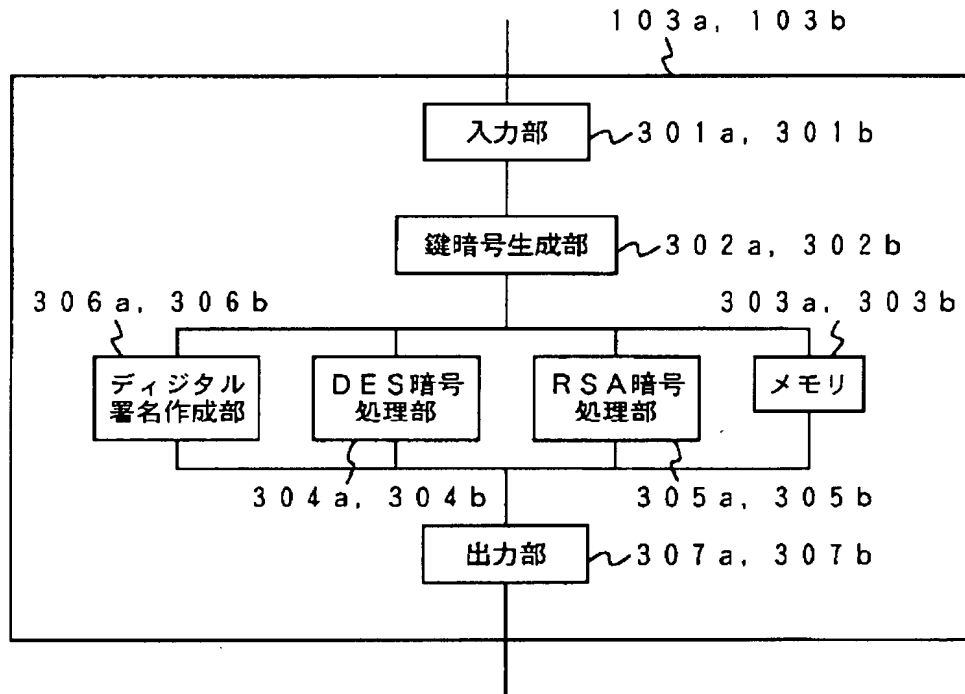
【図2】

ユーザ側装置内部構成（図2）



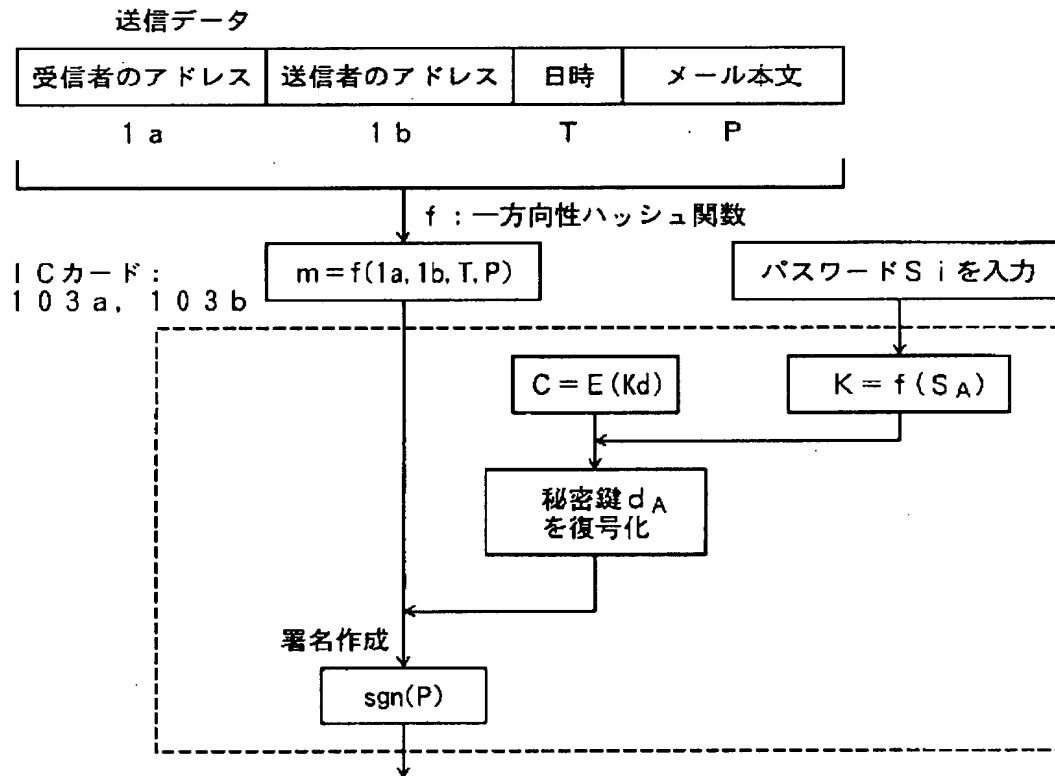
【図3】

ICカード内部構成 (図3)



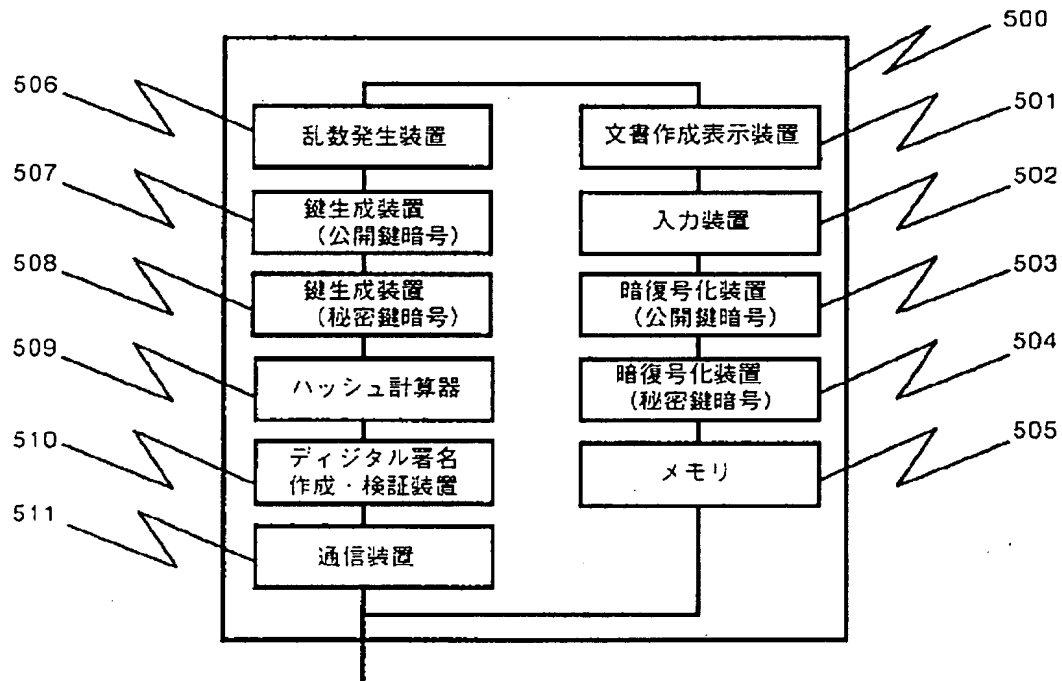
【図 4】

署名作成手順 (図 4)



【図 5】

ユーザ側装置内部構成 (図 5)



フロントページの続き

(51) Int. Cl. ⁶

H 0 4 L 9/32

12/54

12/58

識別記号

庁内整理番号

F I

H 0 4 L 9/00

11/20

技術表示箇所

6 7 3 E

6 7 5 A

1 0 1 B

9466-5K